Enhance Big Data Security in Cloud Using Access Control

Yong Wang
Department of Mathematics and Computer Science
Alcorn State University
Lorrman, MS 39096

Ping Zhang
Department of Mathematics and Computer Science
Alcorn State University
Lorrman, MS 39096

***Abstract*—In this paper, we review big data characteristics and challenges in the cloud. We propose to use access control in data encryption, data segregation, authentication and authorization, identity management, encrypted communication, and fined –grained access. Then we use stochastic process model to conduct security analyses in availability, mean time for security failure and confidentiality failure.**

Keywords—big data; security; cloud; access control

I. INTRODUCTION

When we talk about the cloud computing [11], it includes two sections: the front end and the back end. They connect to each other using computer network, also called Internet. The front end is the user, or client. The back end is the "cloud" section of the system.

The front end has the client's computer and application required to access the cloud computing systems. Not all cloud computing systems have the same user interface. Service includes web-based email programs and web browsers such as Internet Explorer. Other systems embrace applications that provide network service to clients.

As internet becomes popular, big data transactions become a big concern in modern society. The data comes from online business, audios and videos, emails, search queries, health data, network traffic, mobile phone data, and many others [7]. The data is stored in database. The data grows tremendously. The data becomes difficult to store, retrieval, analyze, and visualize using traditional database software to approaches.

In 2012, The human face of big data was compeleted as globe project. The project collects, visualizes, and analyzes big data. For the social network, Facebook has 955 million monthly active accounts in various languages, and 140 billion photos display. The Google support many services with 7.2 billion pages every day. In the next decade, the amount of information managed by the data center will increase by 50 times as estimated. The number of IT professionals will grow by 1.5 times then [8].

There are several kinds of clouding computing based on cloud location, or the service [9]. Based on the service that cloud is offering, there are three kinds of service. These are lassS (Infrastructure as a Service), PaaS (Platform as a service) and SaaS (Software as service). Depending on a cloud location, we can classify clouds as public, private, hybrid, and community cloud.

1.1. *According to NIST Definition for the Clouding Computing, the Service Models are [10]:*

Software as a Service: The service provided to the consumer is to use the provider application running on a cloud infrastructure. The applications are accessible from different client devices through client interfaces. These include web browser or program interface or others. The consumer does not manage or control cloud infrastructure. The infrastructure used in this category includes network, servers, operating systems, and storage.

Platform as a Service (PaaS). The service provided to the consumer is to deploy on cloud infrastructure. The consumer generated or obtained applications using programming languages, libraries, services and tools. The consumer does not manage the cloud infrastructure, which embrace network, services, operating systems, or storage. The consumers do have control the deployed applications and configurations.

Infrastructure as a Service (IaaS). The service provided to the consumer is to provision processing, storage, networks, and other computing resources. The consumer can operate software, operating systems, and application programs. The consumer does not manage cloud infrastructure. The consumer has control on storage, operating systems,, partial network components, and application softwares.

1.2. Cloud deployment models

Public Clouds; Which is most common clouds. Multiple customers can access web applications and services over network. Each individual customer has own resources which are managed by third party vendor. The third party vendor hosts cloud infrastructure for multiple customers from various data centers. The customer has not control how the cloud is managed or what infrastructure is available to them.

Private Clouds: Cloud computing is conducted on private network. They allow users to have cloud computing benefits. The private cloud computing has control over managing data and specify security measurements. This approach result in more user confidence. The disadvantage is that users have high cost because they establish dedicated infrastructure for cloud computing.

Hybrid clouds. Combine both public and private approaches within the same infrastructures. The users will have advantages from both deployments. For instance, the organization can conduct private information on their private cloud and use the public cloud for large traffic.

1.3. *For the cloud, there are five key attributes. These attribute include:*

Multitenancy (Shared resources): Different from previous computing paradigmss, which have dedicated resources and dedicated to single user. Cloud computing relied on business model in which resource are shared through network.

Massive scalability: Cloud computing has ability to scale a large amount of systems. The cloud has ability to scale bandwidth and storage space.

Elasticity: Users can rapidly change their computing resources as needed. The user can release resource for other users when the resources are not needed. In this category, users have a lot of flexibilities.

Pay as you go: Users only pay for the resource applications they actually use and for the time they comsumed.

Self-provisioning of resources: Users self-provision resources alocations. The resources include system and networks.

.

II. BIG DATA CHALLENGES

Big data is large volumes of structured and unstructured data that it is difficult to process using normal database and software. The big data is originated from web searcher organizations who retrieve loosely structured large distributed data.

A. There are five attributes which describe big data [1].

1) *Volume*: many attributes result in increasing volume. These include credit card transaction data, video and audio data, sensor data.

2) Variety: Data are from different formats: normal database, text files, vedio, email communications, and etc.

3) Velocity: data is produced in very fast speed and processed in higher speed.

4) Variability: data can travel in inconsistent speed in different peaks [44].

5) Complexity: data comes from different sources. The data needs to be matched, cleared and changed into specific formats before the process.

B. Based on Elham Abd AL et al. [2], the data security in cloud have the following objectives:

1) Data integrity: it is about data correctness. The data can be changed with authorized person. The system always provide the right data.

2) Data confidentiality: it means that only authorized persons can get the private information. For instance, the medical doctors can access the patient data.

3) Data availability: It means that the electronic systems can provide useful data when the system requires to access. Without availability, the system become useless.

4) Data authentication: It is the process in deciding whether someone or something is declared to be. In general, authentication is performed before authorization

5) Data Storage & Maintenance: Users do not know the data location in cloud environment. It is dynamically stored in the cloud servers. The data in cloud may be exposed to loss or damage because of bad environment or server failure.

a) *Data Breaches and Hacks*: data breach is an important risk in the cloud because of Multi-tenancy.

b) Data separation: Maintain data in isolation.

Data security not only discuss the data encryption, but also support the different policies for data sharing. Resource allocation and memory management need to secure.

C. The data security in cloud can be summarized into network level, user authentication, data level, and generic issues [44].

1) Network level: challenges exists in network level which related to network protocol in TCP/IP, and network security, distributed communications algorithm and distributed data.

2) Authentication level: User authentication level handles encryption/description. Authentication needs to check administration rights for the nodes, users, authentication of different nodes and application logs .

3) Data level: The challenges in data level is related to data integrity and availability. Specifically we encounter data protection and distributed data. Availability is key. Without availability, network security lost its meaning.

4) Generic issues: the challenges are about traditional tools and applications of different technology.

D. Based on survey, there are top ten challenges in big data.

These challenges include three new distinct issues in modeling, analysis, and implementation [12, 13].

Modeling: developing a threat model that covers most of cyber security attacks senarios.

Analysis: discover tractable solution relied on the threat model.

Implementation: develop a solution in the current infrastructure specifically.

Security and privacy are controlled by the three V's of the big data in Velocity, Volume, and Variety. These considerations embrace variables such as large scale cloud infrastructure, diversity of data resources, streaming nature of data acquisition, and high volume of inter-cloud migrations.

The top ten challenges are classified in four categories. These are infrastructure security, data privacy, data management, and integrity and reactive security.

For the infrastructure security, there are secure computation in distributed programming frameworks and secure best practices for non-relation data stores. For the data privacy, there are scalable and composable privacy-preserving data mining and analytics, cryptographically enforced data centric security, and granular access control. For the data management, there are secure data storage and transaction logs, granular audits, data provenance. For integrity and reactive security, there are end-point input validation/filtering, and real time security/compliance monitoring.

Distributed programming frameworks adapt parallelism in computation and storage to process large size of data. One of popular example is MapReduce, which splits an input file into various chuncks. In the first beginning, a Mapper for each chunk reads the data, conduct some computations, and output a list of key/value pairs. In next phase, a Reducer integrates the values belonging to each distinct key and produce outputs.

Non-relational data stores popularized by NOSQL databases are evolving in responding to security infrastructure. The solutions to NOSQL injections are still not mature. Each NOSQL were developed to solve different challenges posed by the analytic world based on our previous knowledge.

Big data can be seen as troubling objects by potentially enabling invasions of privacy, decreased civil freedoms, invasive marketing, and increase state and corporate control in large.

To ensure the most sensitive private data, it is end-to-end secure. The data is only accessible to the authorized persons. Data has to be encrypted based on access control policies. Some research in this area such as attribute-based encryption has to be made more efficient and scalable. To ensure authentication, a cryptographically secure communication approach has to be popularly implemented.

Granular access control is a popular approach in access control. Access control is key to prevent access to data that have some access right. The problem with course-grained access mechanisms is that data that could otherwise be shared. With granular access, data is often changed into a more restricted category in access.

Data and transaction logs are stored in multiple tiered storage media. Manually moving data between tiers provides the IT manager direct control over data. As the data grows exponentially, scalability and availability have pushed several tier levels for big data storage.

Granular audits: With real-time security monitor applications, we try to be notified when an attack take place. To get to the bottom of a missed attack, we need audit information in our observed systems.

Data provenance: Source metadata will grow in complexity because of large origin graphs from programming environments in big data applications. Analysis of such large provenance graphs will detect dependencies for security and confidentiality.

End-point input validation: Many data use cases require data collection from different sources, i.e. end-point device. For example, a security information systems may collect information from millions of hardware device and software applications. A key point of challenges in data collections is input validation.

Real time security/compliance monitoring: Real time security monitoring has always been a challenge in the alerts from devices. These alerts lead to many false positives, which are ignored or simply throw away from our systems.

III. ENHANCE BIG DATA SECURITY USING ACCESS CONTROL

In the following, we propose to use access control to enhance our data security in cloud. Specifically we use access controls in data segregations, authentication and authorization, identification based access control, data encryptions, encrypted communication, and fine-grained access control.

.

3.1.*Data segregation*.

Protecting data integrity, availability and confidentiality is one of challenging task in the cloud computing. The customers data will be preserved and moved from dedicated storage to shared environment by different services providers. It may store in different countries with different police [18]. There are several reasons for security challenges in cloud computing:

1) Because of cloud and dynamic scalability, it is difficult to separate a specific resources in the security breach.

2) It is difficult to arrange unified approach since resources may be owned by various providers.

3) Because of multi-tenancy of cloud that have sharing of resource, the user data may be accessed by unauthorized users.

4) The cloud deals with large amount of information

Based on Subashini and Kavitha [5], multi-Tenancy allows data of different users to reside at the same location. The user data intrusion from the another user is exponently increasing in the environment [6]. In the reality, multi-tenancy is balance between security and cost. The more sharing, more decrease in cost and more increase in utilization. The share will post security risk dramatically [5].

In general, there are three data management approaches:

1) Separate database;
2) Shared database with separate schemas;
3) Shared database with shared schemes.

3.2. *Authentication and Authorization*

In [26], the authors develop a credential classifications and basic structure for analyzing and providing solutions for credential managements that embrace strategies to evaluate the cloud complexity. The study provides a set of analysess for authentication and authorization for the cloud focusing infrastructural organizations. These organizations include

classification for credential and adapt these credentials to the cloud context. The study also provides important factors that need to taken into considerations when presenting a solution for authorization and authentication. For examples, the appropriate requirements, categories, service are identified. In the other aspects, design model for multi factor authentication in the cloud is developed in [27]. The model also provide an analysis for the potential security. Another authentication solution is developed in MILAMob [28].

FemiCloud [29] develops a different approach for authentication and authorization. It applies public key infrastructure (PKI) X.509 certificates for user identification and authentication. FemiCloud is built in OpenNebula, A web interface is used for user management. To avoid the approach limitation, access control lists (ACLs) are used for authorization after successful authentication of users. Authors integrate an local credential mapping service [30].

Tang et al [31] presented collaborative access control properties. These include centralized facilities, agility, homogeneity, and outsourcing trust. They have developed an authorization as a service (AaaS) approach using a formalized multi-tenancy authorization system. The approach also supports administrative control over fine-grained trust models. Integrating trust with cryptographic role based on access control is another solution that support the trust in the cloud [32]. The authors use cryptographic RBAC to enforce authorization policies about the trustworthiness of roles that are evaluated by the data owner. Sander et al. [33] develop a user centric approach for platform-level authorization of cloud services in the OAuth protocol. They allow service to act on behalf of the users when interacting with other services to avoid sharing username and passwords access service.

3.3. *Identity management and access control*

The identity management systems for access control in clouds is discussed in [34]. The authors also present an authorization system for the cloud federation using Shibboleth. Shibboleth is an open source product of the security assertation markup language (SAML) for single sign-on with different cloud approaches. This solution presents how organizations can outsource authentication and authorization to third party solutions using identity management. Stihler et al. [35] also suggest that an integral federated identity management for cloud computing. The trust relationship between a given user and SaaS domain is required so that SaaS users can access the applications and resources. In a PaaS domain, there is an interceptor that acts as a proxy to accept the user ‘s requests and implement them. The interceptor interacts with the secure token service and request the security token using the trust description.

IBHMCC [36] is another solution that has identity-based encryption (IBE) and identity –based signature (IBS) solutions. Relied on the IBE and IBS schemes, an identify-based authentication for the cloud computing has been developed. The approach is depended on the identity-based hierarchical model for the cloud with the corresponding encryption and signatures schemes without using certificates.

Contrail [37] is another way that enhance integration in heterogeneous clouds both vertically and horizontally. Vertical integration supports a unified platform for the different types of resources while horizontal integration abstracts the interaction models of different cloud providers. In [29], the researchers suggest a horizontal federation scheme as a requirement for vertical integration. The developed federation architecture contains several layers in the approaches.

E-ID authentication and uniform access to cloud storage service providers [38] is another approach to build identity management systems for authenticating Portuguese adapt national e-identification cards for the cloud storages. In this trial, the Oauth protocol is integrated with authorization for the cloud users. The e-ID cards contain PKI certificates that are signed by theirl government departments. A certification authority is responsible for e-ID card issues and verifications.
In [39], the authors study inter-cloud federation and the ICEMAN identity management architectures. The ICEMAN integrates identity life cycle, self-service, key management, provisioning that are required in an appropriate inter-cloud identity management system.

3.4. *Data encryption*

If the computer hackers get access to the data, they can get the sensitive information. In general, we want to encrypt all data in cloud. Different data is encrypted using different keys. Without the specific decryption key, the hacker can not get access to sensitive data. In this way, we can limit hacker access to our useful data in cloud.

Amin [14] surveyed how to enhance data security in cloud. They found that the encryption is first choice (45%). A digital signature with RSA algorithm is suggested to protect data security in cloud. Software is used to apply to data documents into few lines using hashing algorithm. These document lines are called message digest. Then software encrypts the message digest with the specific private key to generate the digital signature. Digital signature will be decrypted into digest by own private key and public key of senders to obtain useful information [15].

In [16], RSA algorithm is used to encrypt the data. Biliear Diffe-Hellman enhances the security while having keys exchange. In proposed method, a message header is added to front of each data packet for direct communications between client and cloud without third part server involvement. When users transmit the request to the cloud server for data storage, the cloud server generates public key, private key, and user identification in some server. Two tasks are performed at user end before sending file to cloud. First adds message header to the data and secondly encrypt the data including message headers using specific secret key. When user asks for data for cloud server, it will check received message header and pick up the Unique Identification for Server (SID). If the SID message is found, it will reply to the user requests.

In [17], a technique is introduced to warrant three security attributes in the availability, integrity, and confidentiality. Data in cloud computing uses Secure Socket Layer (SSL) 128 bit encryption that can be raised to 256 bit encryption. The user who wants to access to the data from cloud is required to perform valid user identify and password checks before access is given to encrypted data. In [18], user send the data to the cloud, then cloud service provider provides a key and encrypt the data using RSA algorithm and store into cloud data center. When user requires the data from the cloud, the cloud provider check the authenticity of the user and give the data to the user who can do decryption by computing the private key.

In [19], three layer data security approach is suggested. Each layer conducts various task to make data security in the cloud. The first layer is responsible for authentication, the second layer is responsible for cloud data encryption. And third layer is responsible for data recovery when the cloud fails. In [20], RC5 algorithm is implemented to secure the cloud. A encrypted data is transmitted even if the data is stolen and there will be no corresponding key to decrypt the data. In [21], Role Based Encryption (RBE) is developed to secure data in the cloud. Role based access control (RBAC) cloud architecture was proposed to allow the organizations to store data in the public cloud securely while keeping the secret information of organization's structure in private cloud.

In [22], four authorities are discussed. These include data owners, cloud server, data consumer, and N attribute authorities. For N attributes, authorities sets were divided into N disjoin sets with respect to the category. The data owner get the public key form any one of the authority and encrypt the data before sending it to the cloud server. When data is asked, the authorities will create private key and send it to the data consumer. Consumer will be able to download the file only if he get verified by cloud server.

In [24], location based encryption approach was introduced using user location and geographical position A geographical encryption algorithm was applied on the cloud. The user computer and data was recorded with company name or person who works in the organization. When the data is required, a lot of labels will be searched and retrieved. The information corresponding to the label will be retrieved. In [25], a technique is proposed by using digital signature and Diffie Hellman key exchange in merge with Advanced Encyption Standard encryption algorithm to provide the confidentiality for the data store in cloud.

3.5. *Use encrypted communication when we need to transfer the data.*

For instance, the data can be compromised when we use FTP (file transfer protocol) to transfer data. The communication using the FTP is not encrypted. The hackers can get the information when we transfer data from one place to other. In the contrast, we may use ssl, ssh, or security copy (scp) to transfer data.

3.6. *Fine-grained Access Control.*

Vormetric provides the fine-gained, policy based access controls that restrict access to the data that has been encrypted and allow only autherized access to data by process and users who meet the requirements. The privileged users can read plain texts only if they are approved to do so. The systems update and administrators can see the encrypted data, not plaintext data [13].

IV. SECURITY ANALYSIS

4.1. *Availability and mean time to security failure.*

Wang et al. (2009) have conducted security analysis using stochastic processing. Specifically they applied Multidimentional Markov Process model in security analysis [40, 41].

The Markov process has stationary transition probability if

$$\Pr\{Y_{t+s} = j \mid Y_t = i\} = \Pr\{Y_s = j \mid Y_0 = i\} \quad (1)$$

When a Markov Process has $Y = \{Y_t; t \geq 0\}$ has finite state E and jump times T_0, T_1, … and the imbedded process at the jump time expressed by X_0, X_1, …. , there is a set of scalars $\lambda(i)$ for $i \in E$, called the mean sojourn rates and a Markov matrix P (the imbedded Markov Matrix) that meet the following conditions:

$$\Pr\{T_{n+1} - T_n \leq t \mid X_n = i\} = 1 - e^{-\lambda(i)t} \quad (2)$$

$$\Pr\{X_{n+1} = j \mid X_n = j\} = p(i,j), \quad (3)$$

the analysis is summarized as follows:

I. Identify irreducible sets in the Markov matrix P.

II. Reorder the matrix P so that irreducible and recurrent sets (sits?) on the top, transient states at bottom of the matrix P'.

III. Steady-state analysis for irreducible sets using the following equations

$$\sum_i \pi_i P_{ij} = \pi_j \quad (4)$$

and

$$\sum_j \pi_j = 1 \quad (5)$$

IV $N_T = (I-Q)^{-1}$ for transient states

I is identity matrix. Q is a submatrix associated with the transient states in the Markov matrix P. N_T is number of visits for Markov Chain to the fixed state.

V $F_T(i,j) = 1 - 1/N(j,j)$ if $i = j$ or $F_T(i,j) = N(i,j)/N(j,j)$ (6)

if $i \neq j$, where $F_T(i,j)$ is the first passage probability that Markov chain eventually reaches state j at least once from initial state i.

VI The probability f_k from a transient state i to the kth irreducible set with the sub-matrix b_k can be calculated by:

$$f_k = (I - Q)^{-1} b_k. \quad (7)$$

The Markov process steady-state probability p_j has a relationship with Π_j (the steady-state probability for the imbedded Markov chain) as:

$$p_j = \frac{\pi_j / \lambda_j}{\sum_{k \in E} \pi_k / \lambda_k} \quad (8)$$

When there are different vulnerability attacks existing both in the web server and database server, the system availability can be calculated as:

$$A = 1\text{-}p_{(wsg,sqlf)} - p_{(wsa, sqlf)} - p_{(wsf, sqla)} - p_{(wsf, sqlg)} - p_{(wsf, sqlf)} \quad (9)$$

where (wsg, sqlf), (wsa, sqlf), (wsf, sqlf), (wsf, sqla), and (wsf, sqlg) stand for the different security failure states described in the modeling systems.

As discussed in the method [40, 41], we have Markov matrix P for one-step transition probability in the Markov chain. P can be reorganized as P'

P' =	1				
		1			
			1		
				…	
	b_1	b_2	b_3	…	Q

where b_k is a sub-matrix with the one-step probability of describing transient state i to irreducible set. Sub-matrix Q from the Markov matrix P represents the transition probabilities between the transient states in one-step transition. The mean time to security failure can be calculated using the following operation:

$$N(i,j) = (I - Q)^{-1}(i,j). \quad (10)$$

where N(1,j) is the average number of times the state j ($j \in E_t$) is visited in the Markov chain before the Markov chain arrives at one of the absorbing states from the beginning state.

When we obtain the mean sojourn time in state j (T_j), the mean time for security failure (MTTSF) can be computed by:

$$MTTSF = \sum_{j \in E_t} N_{1j} T_j \quad (11)$$

B. Confidentiality analysis

Confidentiality intrusion tolerance failure in DSDSS occurs when any i ≥ n distributed systems out of n + k - 1 lose their confidentiality [43, 44]. According to B. Madan et al, PCF(i) denote the failure probability of the ith system and P-CF(i) = 1 - PCF(i)

Therefore,

$$PCF = \sum_{i=n}^{n+k-1} \binom{n+k+1}{n} \prod_{j=0}^{i} P_{CF}(j) \prod_{j=1}^{n+k-1-i} \left(1 - \hat{P}_{CF}(i)\right) \quad (12)$$

Since there are $n + k$ replicated copies of a file, loss of confidentiality of just one of these causes loss of confidentiality of the entire system [43,44]. Therefore, system confidentiality failure probability is much greater and is given by,

$$PCF = 1 - \prod_{j=0}^{i} \left(\hat{P}_{CF}(i)\right) \quad (13)$$

ACKNOWLEDGMENT

The authors would like to thank Dr. Bharat Rawal at Penn State University for helps.

REFERENCES.

[1] Narasimha Inukollu, Sailaja Arsi, and Srinvasa Rao Ravuri, . 2014, "Security Issues Associated With Big Data in Cloud Computing,". International Journal of 2014Network Security & Its Application. Vol. 6, No. 3, pp 45-56..

[2] Elham Abd AL, Latif AL Badawi and Ahmed Kayed. 2015." Survey on Enhancing the Data Security of The Cloud Computing Environment By Using Data Segregation Technique,". IJRRAS 23(2), pp 136-143.

[3] Kalana , Parsi, and Sudha Singaraju, 2012," Data security in Cloud Computing Using RSA Algorithm," IJRCCT Vol 1, No 4. Pp 143-146

[4] [4]. Wang, Cong, qian Wang, Kui Ren. And Wenjing Lou. 2010," Privacy-preserving public auditing for data storage security in cloud computing,". In INFOCOM, Proceedings IEEE, pp. 1-9.

[5] Subashini, and V. Kavitha. 2011," A Survey on secutity issues in service delivery models of cloud computing,". Journal of network and computer application, Vol 34, No. 1, pp 1-11.

[6] Almorsy, Mohamed, John Grundy, and Ingo Muller. 2010, An analysis of the cloud computing security problem, In Proceedings of APSEC 2010 Cloud Workshop, Sydney, Austrilia

[7] C. Eaton, D. Deroos, T. Deutsch, G. Lapis, and P. C. Zikopoulos, 2012, Understanding big data: Analytics for Enterprise Class Hadoop and streaming data, MCGraw-Hill Companies.

[8] Big data security, July 2012, Network security, pp.5-8.

[9] P. Mell and T. Grance, September 2011. The NIST Definition of cloud computing. National Institute of Standard and Technology: U. S Department of Commerce. Special publication 800-145.

[10] S Carlin and K, Curran, 2011. Cloud computing security. International Journal of Ambient Computing and Intelligence, 3(1). Pp 14-19.

[11] J. Strickland, How cloud computing works, http://computer.howstuffworks.com/cloud-computing/clopud-computing1.htm (March 2017 access)

[12] E. Sayed, A. Ahmed, and R. A. Saeed. 2014. A survey of big cloud computing.security. International Journal of Computer Science and Software Engineering. Vol 3, No. 1, pp 78-85.

[13] CSA Cloud Security Alliance, 2012 (November), Top ten big data security and privacy challenges.

[14] A. A. Soofi, M. I. Khan, and F. E. Amin, 2014, A review on data security in cloud computing, International Journal of Computer Application. Vol. 94, No. 5, pp12-20.

[15] K. Vamsee, and R. Sriram, 2011. Data security in cloud computing, Journal of computer and mathematicsal science. Vol 2, pp 1-169.

[16] H, Shuai, X. Jianchuan, 2011. Ensuring data storage security through a novel third party auditor scheme in cloud computing. The clouding computing and Imtelligence systems IEEE conference on.

[17] S. K. Sood. 2012, A combined approach to ensure data security in cloud computing. Journal of Network and Computer Applications, 35(6), 1831-1838.

[18] P. Kalpana and S. Singaraju, 2012, Data security in clouding computing using RSA Algorithm. International Journal of Research

in Computer and Communication Technology, Vol. 1, Issue. 4. Pp.1-7

[19] E. M. Mohammed, H. S. Abdelkader, and S. El-Etriby, 2012, Enhanced data security model for cloud computing. International conference on Information and Systems.

[20] J. Singh, B Kumar, and A. Khatri. 2012, Improving store data security in cloud using RC5 algorithm.

[21] Z. Lan, V. Varadharajan, M. Hitchens, 2013, Achieving Secure Role=based Access Control on Encrpted Data in Cloud Storage. Information Forensic and Security, IEEE Transaction on , 8(12): 1947-1960.

[22] J. Tacho, L. Xiang-Yang, Zhioguo Wang, and W. Meng, 2013. Privacy preserving cloud data access with multiple authorities, INFOCOM, proceeding of IEEE, pp. 14-19.

[23] Y. Ching-Nung, and L. Jia-bin, 2013, Protecting Data Privacy and Security for Cloud Computing Based on Secret Sharing, International Symposium on the Biometrics and Security Technologies.pp.1-7

[24] M. S. Abolghasemi, M.M. Sefidab, R. E. Atani, 2013. Using location based encryption to improve the security of data access in cloud computing, International Conference on Computing, Communications, and Informatics.

[25] P. Rewagad, and Y. Pawar, 2013, Use of digital signature with Diffie Hellman key exchangeand AES algorithm to enhance data security in cloud computing. International Conference on the communication systems and Network Technologies.

[26] N. Mimura Gonzalez, M. Torrez Rojas, Maciel da Silva, F. Redigolo, T. Melo de Brito Carvalho, C. Miers, M. Naslund, and A. Ahmed, A Framwork for authenitication and authorization credential in cloud computing, 2013, 12th International Conference in Trust, Security and Privacy in computing and communication, pp. 509-516.

[27] R. Banyal, P. Jain, and V. Jain, 2013, Multi-factor authentication framework for loud computing in Fifth International Conference on Computational Intelligence, Modeling and Simmulation. Pp 105-110

[28] R. Lomotey, and R. Deters, 2013, Saas authentication middleware for mobile consumers of iaas cloud, IEEE Ninth World Congress on Services, pp 448-455.

[29] H. Kim, and S. Timm, 2014, X.509 Authentication and Authorization in femi cloud. IEEE/ACM 7th International Conference on Utility and Cloud Computing. Pp 732-737.

[30] A. Gholami, and E. Laure, 2015, Security and Privacy of Sensitive Data in Cloud Computing: A Survey of Recent Development, Computer Science and Information technology.

[31] B. Tang, R. Sandhu, and Q. Li, 2013, Multi-tenancy Authorization Model for Collaborative Technologies and Systems. Pp 132-138.

[32] L. Zhou, V. Varadharajan, and M. Hitchens, 2013, Integrating trust with cryptographic role based access control for secure data storage. In Trust, Security, and Privacy in Computing and Communications. 12th IEEE International Conference on, pp 560-569.

[33] J. Sendor, Y. Lehmann, G. Serme, A. Santana de Oliveira, 2014, Platform level support for authorization in cloud services with oauth2, IEEE International Conference on Cloud Engineering , pp458-465.

[34] M. A. Leandro, T. J. Nascimento, D. R. Dos Santos, C. M, Westphall, 2012, Multitenancy authorization system with federated identify for cloud-based environments using Shibboleth, the 11th International Conference on Networking, pp 88-93.

[35] M. Stihler, A. Santin, A. Marcon, and J. Fraga, 2012, Integral federated identityty management for cloud computing, In new Technologies, Mobility and Secuiry, 5th International Conference on, pp. 1-5.

[36] H, Li, Y. Dai, L. Tian, and H. Yang, 2009, Identity-based authentication for cloud computing, in Cloud Computing (M. Jaatun, G. Zhao, and C Rong. Eds). Vol 5931 Lecture Notes in Computing Science, pp. 157-166.

[37] E. Carlini, M. Coppola, P. Dazzi, L. Ricci, and G. Righetti, 2012, Loud federation in contail, in Europar 2011: Parallel Processing Workshops (M. Alexander, P. D' Ambra, A. Belloum, S. Scott, J. Cannataro, M. Danelutto, B. Di Mar tino, M. Gerndt, E. Jeannot, R. Namyst, J. Roman, S. Scott, J. Traff, G. Vallee, and J. Weidendorfer, eds). Vol 7155 Lecture Notes in Computer Science, pp.159-168.

[38] J. Gouveia, P. Crocker, S. Melo De Sousa, and R. Azevedo,2013, E-id authenticationand uniform access to cloud storage service providers, in Cloud Computing Technology and Science, IEEE 5th Conference on, Vol. 1, pp.487-492.

[39] G. Dreo, M. Golling, W. Hommel, and F. Tietze,2013, Iceman: An architecture for secure federated inter-cloud identity management , in Integrated Network Management , IFIP/IEEE International Symposium on, pp1207-1210.

[40] Y. Wang , W. M. Lively, and Simmons D. B. Software security analysis and assessment for web-based applications. *Special Issue of Journal of Computational Methods in Science and Engineering* 2009; pp. 179-190.

[41] R M Feldman, and Valdez-Flores C, Applied probability and stochastic processes, 2nd Edition, PWS Publishing Company, St. Paul, MN; 2006.

[42] S. Ross, Stochastic Processes, 2nd edition, John and Willey Sons Inc.1996.

[43] Wang, Dazhi, Madan Bharat B, and Trivedi Kishor S. Security analysis of SITAR intrusion tolerance system. In Proceedings of the 2003 ACM workshop on Survivable and self-regenerative systems: in association with 10th ACM Conference on Computer and Communications Security. 2003. pp. 23-32.

[44] Bharat S. Rawal, Harsha K. Kalutarage, S. Sree Vivek and Kamlendu Pandey, "The Disintegration Protocol: An Ultimate Technique for Cloud Data Security," 2016 IEEE International Conference on Smart Cloud,